ﾉ

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/016,740	10/30/2001	Gregory C. Kime	42390P12158	5450

8791 7590 08/11/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
STRANGE, AARON N	
ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 08/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/016,740	**Applicant(s)** KIME ET AL.	
	Examiner Aaron Strange	**Art Unit** 2153	

-- The MAILING DATE of this communication appears on the cover she t with the correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *31-36,39-46,48-53 and 58-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *31-36,39-46,48-53 and 58-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 5/22/2006 have been fully considered but they are not persuasive.

2. With regard to claim 31, and Applicant's assertion that Rajasekharan does not teach or suggest that a "unique validation key is generated based on ...an encryption key", since "a digital signature being an DSA or RSA signature is not the same as a unique key being generated based on ...encryption key", the Examiner respectfully disagrees.

Rajasekharan discloses that a unique validation key (source indicator) is generated based on an encryption key, since the source indicator may be a digital signature such as a DSA or RSA signature. For example, it is well known that DSA signatures use an encryption key (private key) to generate the signature. Clearly, the unique validation key, which may be a DSA signature is generated "based on an encryption key".

3. With further regard to claim 31, and Applicant's assertion that Adbulhayogu does not disclose that "a unique validation key is generated based on ... a uniform resource location (URL)", since " a digital signature that includes a URL is not the same as a unique key being generated based on a URL", the Examiner respectfully disagrees.

Generation of a key containing a URL clearly necessitates generation of the key based on the URL, since a change in the URL will result in a change in the key.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-36,39-41,44-46, 48-51, and 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rajasekharan et al. (US 6,480,961) in view of Xie et al. (US 6,606,393).

6. With regard to claim 31, Rajasekharan discloses a method for validating a data stream comprising:

generating a unique validation key associated with the data stream (source indicator), the unique validation key to map the data stream with a source (Col 5, Lines 28-38), wherein the unique validation key is generated based on an encryption key (digital signature is generated using DSA/RSA)(Col 4, Lines 25-27 and Col 5, Lines 27-29);

generating the data stream (data stream is sent)(Col 4, Lines 51-55);

storing the unique validation key (authorization data is stored at server)(Col 4, Lines 8-12); and sending the unique validation key (authorization data is sent to client)(Col 4, Line 6) and data stream (Col 4, Lines 51-55) to a destination (client). Rajasekharan fails to disclose embedding the validation key in the data stream to form a validation key embedded data stream or that the validation key is generated based on a URL.

Xie discloses several methods of authenticating digital messages that are old and well known in the art. Xie further discloses that embedding validation information within the digital stream is advantageous since removal of embedded information may destroy or alter the content. This provides better security that sending the validation data outside of the data stream (Col 1, Lines 27-45).

Abdulhayoglu discloses a similar system for verifying the source of received data based on a digital certificate included with the data. Abdulhayoglu teaches use of a digital certificate that includes a URL of the data source (¶84). This allows the recipient to verify that the source of the data is at that URL. This would have been an advantageous addition to the system disclosed by Rajasekharan, since it would have allowed a recipient of the data stream to be assured that the URL from which the data stream is coming is the URL that was requested.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the validation key based on the URL of the data source and embed the validation key in the data stream to form a validation key embedded data stream in order to provide enhanced security since embedded validation keys would be much more difficult to remove from the data stream without corrupting it, ensuring that the source and URL could be validated by the recipient of the data stream.

7. With regard to claim 32, Rajasekharan further discloses that the source is any one of a source of audio information, video information, audio-video information and the URL (Col 4, Lines 1-2).

8. With regard to claim 33, Rajasekharan further discloses that generating the validation key associated with the data stream comprises generating the unique validation key in response to a request for data to be retrieved from the URL. Since the source of the unique validation key is a server computer accessed via the Internet (Col 4, Lines 6-9), it must be accessed via a URL prior to sending the authorization data to the client.

9. With regard to claim 34, Rajasekharan further discloses that generating the unique validation key associated with the data stream, said unique validation key to map the data stream with a source, comprises: generating the unique validation key (Col 5, Lines 28-38) and sending the unique validation key to the destination (Col 4, Line 6).

10. With regard to claim 35, Rajasekharan further discloses that the data stream comprises any one of encoded video information, encoded audio information, encoded audio-video information, and encoded information from the URL (Col 4, Lines 1-2).

11. With regard to claim 36, Rajasekharan further discloses receiving the validation key at the destination (Col 4, Line 6); sampling the unique validation key embedded data stream at the destination to detect the unique validation key (validation key is detected and checked) (Col 4, Lines 24-28).

12. With regard to claim 39, Rajasekharan discloses:

receiving a unique validation key associated with the data stream (Col 4, Line 4), the unique validation key to map the data stream with a source (Col 5, Lines 28-38); receiving the data stream (Col 4, Lines 51-52), wherein the unique validation key is generated based on an encryption key (digital signature is generated using DSA/RSA)(Col 4, Lines 25-27 and Col 5, Lines 27-29);

detecting the unique validation key and validating the data stream in response to detecting the validation key (key is detected and checked)(Col 4, Lines 24-28). The validation key must be stored since the client receives it and analyzes it. Rajasekharan fails to disclose that the validation key is embedded in the data stream or that the validation key is generated based on a URL.

Xie discloses several methods of authenticating digital messages that are old and well known in the art. Xie further discloses that embedding validation information within the digital stream is advantageous since removal of embedded information may destroy or alter the content. This provides better security that sending the validation data outside of the data stream (Col 1, Lines 27-45).

Abdulhayoglu discloses a similar system for verifying the source of received data based on a digital certificate included with the data. Abdulhayoglu teaches use of a digital certificate that includes a URL of the data source (¶84). This allows the recipient to verify that the source of the data is at that URL. This would have been an advantageous addition to the system disclosed by Rajasekharan, since it would have allowed a recipient of the data stream to be assured that the URL from which the data stream is coming is the URL that was requested.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the validation key based on the URL of the data source and embed the validation key in the data stream in order to provide enhanced security since embedded validation keys would be much more difficult to remove from the data stream without corrupting it, ensuring that the source and URL could be validated by the recipient of the data stream.

13. With regard to claim 40, Rajasekharan further discloses that the source is any one of a source of audio information, a source of video information, a source of audio-video information and the URL (Col 4, Lines 1-2).

14. With regard to claim 41, Rajasekharan further discloses requesting data to be retrieved from the URL. Since the source of the validation key is a server computer accessed via the Internet (Col 4, Lines 6-9), it must be accessed via a URL prior to sending the authorization data to the client.

15. Claims 42,43,52,53, and 55-56 are rejected under 35 U.S.C. 103(a) as being unpatentable Rajasekharan et al. (US 6,480,961) in view of Xie et al. (US 6,606,393) in further view of Willis, Jr. et al. (US 6,738,815).

16. With regard to claims 42,43,52, and 53, while the system disclosed by Rajasekharan in view of Xie shows substantial features of the claimed invention (discussed above), it fails to disclose generating an error if the unique validation key is not detected in the data stream or writing the error to a log file. Rajasekharan does disclose checking the validation key to determine is the source is an authorized source (Col 4, Lines 24-28). Xie discloses that removing embedded validation keys may destroy or at least damage the underlying data (Xie, Col 1, Lines 36-36)

Willis, Jr. teaches the creation of a log file at a client and writing errors to the log file when they occur (Col 6, Lines 44-50). Willis, Jr. further discloses that the logs can be uploaded to a server as well (Col 6, Lines 49-50). This would have been an advantageous addition to the system disclosed by Rajasekharan in view of Xie since generating an error and storing it in a log file would have allowed the server, client, and/or users to be notified that the validation key was not found, and that the data may be invalid.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate an error and write it to a log file if the validation data is not detected in the data stream. This would have allowed the server, client, and/or users to be notified that the validation keys were not found and that the data may be invalid.

17. Claims 44-46 and 48 are rejected for the same reasons cited above regarding claims 31,32,35, and 33, respectively, since they recite substantially identical subject matter. A database is required in order to store the validation key at the server, and is therefore inherent. A processor and memory are inherent components of both the server and client devices since they are computers.

18. Claims 49 and 50 are rejected for the same reasons cited above regarding claims 31 and 32, respectively, since they recite substantially identical subject matter. A bus, processor, and memory containing instructions are inherent components of both the server and client devices since they are computers.

19. With regard to claim 49, Rajasekharan discloses a system comprising:

a key generation module (KGM) to generate a unique validation key associated with a data stream (source indicator), the unique validation key to map the data stream with a source (Col 5, Lines 28-38), wherein the unique validation key is generated based on an encryption key (digital signature is generated using DSA/RSA)(Col 4, Lines 25-27 and Col 5, Lines 27-29);

a client to receive the validation key and data stream (Col 4, Line 6);

and a database couples with the client to store the unique validation key (client stores validation key to perform periodic checks) (Col 4, Line 65 to Col 5, Line 3). Rajasekharan fails to disclose embedding the validation key in the data stream to form a validation key embedded data stream or that the validation key is generated based on a URL.

Xie discloses several methods of authenticating digital messages that are old and well known in the art. Xie further discloses that embedding validation information within the digital stream is advantageous since removal of embedded information may destroy or alter the content. This provides better security that sending the validation data outside of the data stream (Col 1, Lines 27-45).

Abdulhayoglu discloses a similar system for verifying the source of received data based on a digital certificate included with the data. Abdulhayoglu teaches use of a digital certificate that includes a URL of the data source (¶84). This allows the recipient to verify that the source of the data is at that URL. This would have been an advantageous addition to the system disclosed by Rajasekharan, since it would have allowed a recipient of the data stream to be assured that the URL from which the data stream is coming is the URL that was requested.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the validation key based on the URL of the data source and embed the validation key in the data stream in order to provide enhanced security since embedded validation keys would be much more difficult to remove from the data stream without corrupting it, ensuring that the source and URL could be validated by the recipient of the data stream.

20. With regard to claim 50, Rajasekharan further discloses that the source is any one of a source of audio information, video information, audio-video information and the URL (Col 4, Lines 1-2).

21. With regard to claim 51, Rajasekharan further discloses that the client requests data to be retrieved from the URL. Since the source of the data is a server computer accessed via the Internet (Col 4, Lines 6-9), it must be accessed via a URL prior to sending the data stream to the client.

22. Claims 58 and 60 are rejected for the same reasons cited above regarding claims 31 and 35, respectively, since they recite substantially identical subject matter. A machine-readable medium containing instructions to perform the methods is inherent in the system disclosed by Rajasekharan since the system is implemented using computers.

23. With regard to claim 59, Rajasekharan further discloses sampling the data stream to detect the unique validation key embedded in the data stream (Col 4, Lines 24-28).

Conclusion

24. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aaron Strange whose telephone number is 571-272-3959. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess can be reached on 571-272-3949. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AS
8/6/2006

GLENTON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100